IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
SAMSUNG SD CARD FOR MICRO SD LOT NUMBER 20170928	MAGISTRATE NO. 18-1741M **[UNDER SEAL]**
LACIE EXTERNAL HARD DRIVE SERIAL NUMBER NL3155Q	MAGISTRATE NO. 18-1742M **[UNDER SEAL]**
MAC BOOK PRO LAPTOP COMPUTER SERIAL NUMBER C02RTL8TFVH3	MAGISTRATE NO. 18-1743M **[UNDER SEAL]**
SCAN DISK ULTRA 64GB THUMB DRIVE IDENTIFYING NUMBER BN160625619B	MAGISTRATE NO. 18-1744M **[UNDER SEAL]**
ILOK THUMB DRIVE IDENTIFYING NUMBER 0018BC1F	MAGISTRATE NO. 18-1745M **[UNDER SEAL]**
PINK COLORED APPLE IPHONE S MODEL A1633 FCCID BCG-E2946A IC:579C-E2946A	MAGISTRATE NO. 18-1746M **[UNDER SEAL]**
BLACK S9 SAMSUNG GALAXY IMEI: 353309091921724 FCCID: A3LSMG96OU	MAGISTRATE NO. 18-1747M **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Michael P. Radens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search certain electronic devices currently in the possession of the United States Secret Service, specifically as follows: Samsung SD Card for Micro SD Lot number 20170928; LaCie External Hard Drive serial number NL3155Q; Mac Book Pro Laptop Computer serial number C02RTL8TFVH3; Scan Disk Ultra 64GB Thumb drive identifying number BN160625619B; ILok Thumb Drive identifying number 0018BC1F; Pink colored Apple iPhone S Model A1633 FCCID: BCG-E2946A IC:579C-E2946A; Black S9 Samsung Galaxy

IMEI: 353309091921724 FCCID: A3LSMG96OU. This application seeks permission to search these electronic devices, further described in Attachment A, for the things described in Attachment

2. I am a Special Agent with Homeland Security Investigations (HSI) and have been since July of 2011. I am currently assigned to the Pittsburgh Office and am trained and authorized to investigate offenses such as are alleged herein. I have received training at the Federal Law Enforcement Training Center in the investigation of financial crimes.

3. Prior to my employment with HSI, I was employed as a Special Agent with the United States Secret Service from 2006 to 2011. While with the Secret Service I received training in credit card fraud, and identity theft. I have investigated multiple individuals engaged in the production and use of counterfeit identification documents and counterfeit credit cards.

4. As a federal agent, I am authorized to investigate violations of the laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. The statements contained in this Affidavit are based primarily on information gathered by me and other agents of the United States Postal Inspection Service, as well as my personal knowledge, observations, experience and training, review of documents and records, and discussions with other law enforcement agents.

PROBABLE CAUSE

6. On December 3, 2018, your Affiant, a member of the Financial Crimes Task Force of Southwest Pennsylvania, was contacted by the Plum Borough Police Department (PBPD) concerning the arrest of Florida residents Christopher Joseph TYRELL and Nigel Rakeem JOHNSTON. On November 21, 2018 the PBPD seized multiple fraudulent identification documents and approximately 80 fraudulent Discover Card account numbers located on approximately 40 counterfeit credit cards possessed by TYRELL and JOHNSTON. Other items were also seized including marijuana, a laptop computer, cell phones and external electronic

storage media. TYRELL and JOHNSTON were subsequently charged by the PBPD for credit card fraud, false identification and identity theft related violations of the Pennsylvania Crimes Code including Section 4106 for Access Device Fraud, Section 3922 for Theft by Deception, Section 7614 for Unlawful Duplicating, Section 4104 for Tampering With Records of Identification, Section 4120 for Identity Theft, Section 4101 for Forgery, Section 4914 False Identification to Law Enforcement Authorities, and Section 0903 for Criminal Conspiracy as well as additional violations. The PBPD requested the assistance of your Affiant with the investigation.

7. On November 21, 2018 at approximately 00:21 hours PBPD Officer Rupert observed a dark colored Kia sedan running with no head lights parked near the Sunoco Gas Station located at 255 Unity-Center Road in Plum Borough, Pennsylvania. The vehicle displayed a Florida registration CTDL93 and was occupied by two individuals. Officer Rupert made contact with the individuals and identified them as TYRELL and JOHNSTON. Officer Rupert determined the vehicle was a Hertz rental car rented to Aquil JOHNSTON, who was not present in the vehicle. Neither TYRELL or JOHNSTON had a phone number to contact Aquil JOHNSTON concerning the rental vehicle, which was past due for its return to Hertz.

8. After Officer Rupert learned that the vehicle was past due, TYRELL and JOHNSTON were asked to step out of the vehicle. JOHNSTON, the driver of the vehicle was removed first and consented to a pat down of his person by Officer Rupert. TYRELL, the vehicle passenger, was also removed from the vehicle and consented to a search of his person. Officer Rupert located a black wallet in the front right pocket of TYRELL. Upon police locating the wallet TYRELL spontaneously uttered "Fuck". A search of the wallet revealed 5 different State ID documents in several different names. Five Discover Card credit cards with names other than TYRELL and JOHNSTON were also located within the wallet. TYRELL was immediately deemed "John Doe" based on the discovery of multiple ID documents by the PBPD and placed in a patrol vehicle. TYRELL (John Doe) was later positively identified as Christopher TYRELL.

9. After the PBPD advised JOHNSTON why TYRELL was in custody, JOHNSTON verbally consented to a search of the vehicle. The PBPD located several marijuana seeds behind the driver's seat. JOHNSTON stated the black bag which was located by Police in the vehicle was his. The PBPD located drug paraphernalia within the bag. The PBPD stopped their search of the vehicle and requested a K9 Officer to the scene to perform an exterior sweep of the vehicle. The K9 Officer advised that the dog had alerted to the rear of the vehicle where JOHNSTON's bag was located, as well as the trunk of the vehicle. JOHNSTON was also placed in custody and the rental vehicle was towed and placed in a secure location.

10. Upon arriving at the Plum Borough Police Station Detective Ken Farmerie advised TYRELL and JOHNSTON of their Miranda Rights. TYRELL refused to answer questions at that time. JOHNSTON stated he and TYRELL had traveled from Akron, Ohio, earlier that day but did not provide a reason for the trip. JOHNSTON stated he had smoked marijuana prior to leaving Akron. When asked if there was anything illegal in the vehicle JOHNSTON stated there was an ounce of marijuana in the car.

11. Continuing on November 21, 2018, the PBPD obtained a search warrant for the Hertz rental vehicle occupied by TYRELL and JOHNSTON from Plum Magistrate District Judge Zucco.

12. Upon execution of the search warrant, numerous items were located by the PBPD within the vehicle, including the items described in Attachment A of this affidavit: Samsung SD Card for Micro SD Lot number 20170928; LaCie External Hard Drive serial number NL3155Q; Mac Book Pro Laptop Computer serial number C02RTL8TFVH3; Scan Disk Ultra 64GB Thumb drive identifying number BN160625619B; ILok Thumb Drive identifying number 0018BC1F; Pink colored Apple iPhone S Model A1633 FCCID: BCG-E2946A IC:579C-E2946A; Black S9 Samsung Galaxy IMEI: 353309091921724 FCCID: A3LSMG96OU.

13. One Discover Card credit card (X8883) was located in JOHNSTON's black bag located within the vehicle. Five Discover Card credit cards (X7027; X4076; X7292; X0927; X2034) were located in the black wallet owned by TYRELL. An additional 34 Discover Card credit cards were located in TYRELL's black bag located in the trunk of the vehicle.

14. On December 6, 2018, your Affiant and United States Postal Inspector Dave Anderchak responded to the PBPD to provide assistance with the investigation. Your Affiant visually inspected the 40 Discover Card credit cards and immediately identified white edges on some but not all the credit cards indicating inconsistent printing. Based on your Affiant's knowledge and experience with counterfeit credit card investigations, the appearance of the white edges indicated that the cards were not properly printed and therefore may be fraudulently manufactured.

15. Your Affiant and Detective Farmerie used a magnetic stripe card reader to compare the account number embossed (raised) on the front of the credit card to the track data, which includes the credit card account number encoded on the magnetic stripe located on the rear of the credit card. Investigation revealed that the numbers embossed on the front of the credit cards were different than the numbers encoded on the magnetic stripes, confirming the cards were in fact counterfeit. All of the account numbers embossed on the cards, as well as the account numbers located on the magnetic stripes, are in fact Discover Card credit card accounts beginning with the 4-digit sequence 6011.

16. It is of note that, for all but one of the counterfeit cards, the last four digits of the account number embossed on the front of the card matched the last four digits of the account number encoded on the magnetic stripe, even though the full account numbers were different. This is done by the fraudster so that the last four digits printed on any receipt by a victim retailer will match the embossed number on the front of the credit card. On the remaining counterfeit card, the

last four digits of the embossed number and the last four digits of the magnetically encoded number did not match.

17. That same day, Inspector Anderchak provided Discover fraud investigators with a preliminary list of the victim account numbers. Preliminary results indicate approximately $50,000 in loss to Discover resulting from approximately 140 fraudulent transactions.

18. PBPD located an Ohio Turnpike toll receipt for $6.25 within TYRELL and JOHNSTON's rental vehicle dated November 20, 2018 at 22:16, only a few hours before their encounter with the PBPD. The toll was paid with a credit card ending in X7027. It is of note that the credit card found in the wallet of TYRELL was embossed with the last four digits X7027. Based on track data recovered after swiping the Discover card ending in X7027, investigators believe the true owner of the account number used to pay the toll is an individual with initials D.B. This account number has not yet been provided to Discover, indicating that losses in the case will increase.

19. The PBPD identified three counterfeit identification documents in TYRELL's wallet: one Ohio driver's license with the name Justin Palmer DL#RR287135, and two South Carolina driver's licenses, one in the name Courtney Walker DL#104170172 and another in the name Curtis Bailey DL#104170172. Both of the South Carolina ID cards indicate the same driver's license number, indicating both are counterfeit. The same photo of TYRELL is present on all three of the licenses. The name Courtney Walker is embossed on numerous counterfeit Discover Card credit cards indicating TYRELL planned to use the Walker ID document when uttering the counterfeit credit cards.

20. Detective Farmerie informed your Affiant that after TYRELL and JOHNSTON arrived at the Plum Borough Police Department, the pink colored Apple iPhone S belonging to TYRELL received numerous unanswered telephone calls. Officers observed the incoming calls were received from a number saved in the phone as "Discover". Based on your Affiant's

knowledge and experience of working credit card fraud investigations, the number saved in the phone as "Discover" may have been the source of the counterfeit cards, or other unidentified coconspirators working with TYRELL and JOHNSTON attempting to contact them via the cell phone.

21. Your Affiant notes that the PBPD's encounter with TYRELL and JOHNSTON occurred in close proximity of a Sunoco Gas Station. Based on your Affiant's knowledge and experience, individuals that traffic in stolen credit cards often obtain credit card account numbers through the use of gas pump skimming devices. Although no skimmers were retrieved from the Sunoco Gas Station, the card readers were not inspected until December 12, 2018, several days after TYRELL and JOHNSTON were arrested. Your Affiant visually inspected several of the pumps on December 12, 2018, noting one of the card readers at the station had begun to malfunction and was out of order. The card reader may have been damaged as the result of the installation or removal of a "Deep Insert" skimming device removed after the individuals were arrested but prior to the inspection of the pumps. On December 9, 2018 the PBPD received a report from a victim with initials C.B., a resident of Plum Borough. The individual stated her Dollar Bank credit card was used at the same Sunoco Gas Station on Unity-Center Road. She provided information that her card was fraudulently used in North Randel Ohio and Maple Heights Ohio after the use at the Sunoco, indicating a skimming device may previously have been present.

22. Your Affiant also knows through training and experience, as well as from the investigation of TYRELL and JOHNSTON, that the conspirators in this access device fraud and identity theft conspiracy communicated by electronic means. Electronic devices such as computers, tablets, cell phones or other electronic storage devices can store thousands of pieces of data, and are often used to produce counterfeit credit cards. Their storage capacity can also be used to store credit card account information and identification documents. Based on the calls from "Discover," TYRELL and JOHNSTON were more likely than not in communication with

unidentified coconspirators via their cellular devices. The external storage devices including the laptop computer, external hard drive, SD Card, two thumb drives and cell phone have the capability to store massive amounts of credit card account numbers, photos, personally identifiable information (PII), and are all often utilized in the process of manufacturing counterfeit credit cards and identification documents, which were all possessed by TYRELL and JOHNSTON.

23. Based on your Affiant's knowledge and experience, counterfeit credit cards like the cards seized in this investigation are manufactured through the use of a computer and a Magnetic Stripe Reader / Writer Device (MSR), which is used to alter or encode track data located on the magnetic stripe of a credit card. The MSR software is easily identified on computer devices even in cases were the MSR is not recovered as evidence.

24. Therefore, your Affiant has reason to believe that within the electronic devices there is evidence concerning the production and distribution of counterfeit credit cards and identification documents.

25. The devices are currently in the lawful possession of the United States Secret Service in Pittsburgh, Pennsylvania. All of the items (Samsung SD Card for Micro SD Lot number 20170928; LaCie External Hard Drive serial number NL3155Q; Mac Book Pro Laptop Computer serial number C02RTL8TFVH3; Scan Disk Ultra 64GB Thumb drive identifying number BN160625619B; ILok Thumb Drive identifying number 0018BC1F; Pink colored Apple iPhone S Model A1633 FCCID: BCG-E2946A IC:579C-E2946A; Black S9 Samsung Galaxy IMEI: 353309091921724 FCCID: A3LSMG96OU) were transferred to Homeland Security Investigations and the United States Postal Inspection Service by the Plum Borough Police Department, and were in turn provided to the computer forensic examiners at the United States Secret Service. Homeland Security Investigations, the United States Postal Inspection Service, and the United States Secret Service are currently members of the Financial Crimes Task Force of

Southwest Pennsylvania and collaborate to investigate financial frauds throughout the Western District of Pennsylvania.

26. The device are currently in storage at 112 Washington Place, 2 Chatham Center, Suite 1610, Pittsburgh, PA 15219. In my training and experience, I know that the devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of Homeland Security Investigations.

TECHNICAL TERMS

27. Based on my training and experience, I use the term "wireless telephone" to convey the following meaning. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

28. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.apple.com/iphone/iphone-4/specs.html, I know that the cellular telephones for which these search warrants are sought have capabilities that allow them to serve as wireless telephones,

digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. There is probable cause to believe that things that were once stored on the electronic devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices because:

a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

34. I submit that this Affidavit supports probable cause for a search warrant authorizing the search of the electronic devices described in Attachment A, and to seize the items described in Attachment B.

35. Based on my training and experience, and the facts set forth in this Affidavit, there is probable cause to believe that there is evidence of Access Device Fraud, Identity Theft, and Criminal Conspiracy contained within the electronic devices seized from Christopher TYRELL and Nigel JOHNSTON, as described in Attachment A.

REQUEST FOR SEALING

36. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Michael P. Radens, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on December 21, 2018:

HONORABLE MAUREEN P. KELLY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Items to be Searched

The device described below is currently located at the evidence storage room at 112 Washington Place, 2 Chatham Center, Suite 1610, Pittsburgh, PA 15219. The electronic device to be searched is:

a. a Samsung SD Card for Micro SD Lot number 20170928

This warrant authorizes the forensic examination of the electronic devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Items to be Seized

1. All records relating to violations of Title 18, Sections 1028 (Identity Theft), 1029 (Access Device Fraud) and 371 (Conspiracy) occurring prior to November 21, 2018;

2. Any and all records and information relating to the production and trafficking of skimming devices;

3. Any and all records and information relating to the production, purchase, sale or trafficking in counterfeit credit cards, counterfeit access devices, and counterfeit identification documents;

4. Any and all records and information relating to communications between and among Christopher Tyrell and Nigel Johnston or any other conspirator concerning the trafficking and use of counterfeit access devices, counterfeit credit cards and counterfeit identification documents;

5. Any and all records and information relating to financial records, books, notes, lists of credit card accounts, track data, or photographs concerning the production or trafficking of counterfeit access devices and counterfeit identification documents;

6. Any and all records and information relating to equipment and materials used in the production of counterfeit identification documents and counterfeit access devices including white plastic cards, printing equipment, cameras, holograms, foil, magnetic stripe reader/writers, and device-making equipment;

7. Computers or storage media used as a means to commit the violations described above;

8. For any wireless or cellular telephone whose search is authorized by this warrant, records and information described above may be seized in any format, including:

a. incoming and outgoing call and text message logs;

b. contact lists;

c. photo and video galleries;

d. sent and received text messages;

e. online searches and sites viewed via the Internet;

f. online or electronic communications sent and received, including email, chat, and instant messages;

g. sent and received audio files;

h. navigation, mapping, and GPS files;

i. telephone settings, including speed dial numbers and the telephone number for the subject telephone and related identifying information such as the ESN for the telephone;

j. call forwarding information;

k. messages drafted but not sent;

l. voice messages;

9. For any computer or storage medium whose search is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

10. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.